

FIG. 1

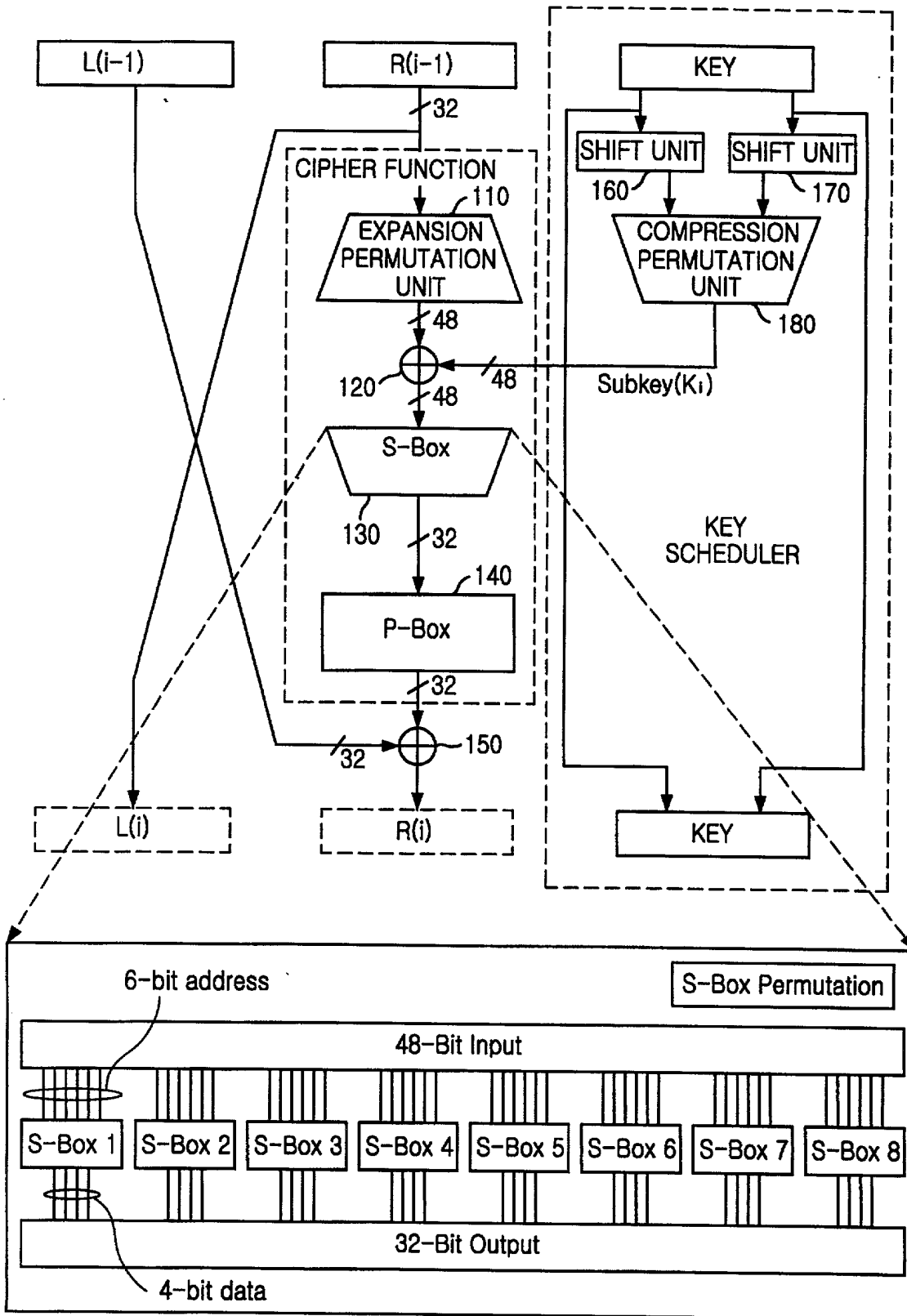


FIG. 2

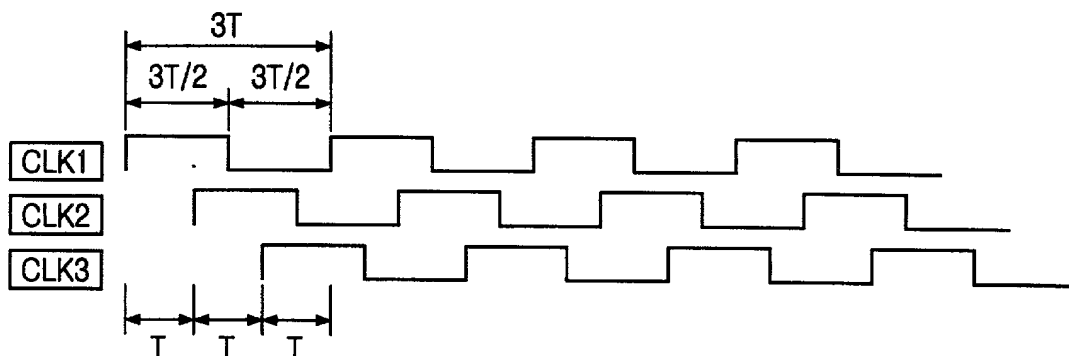
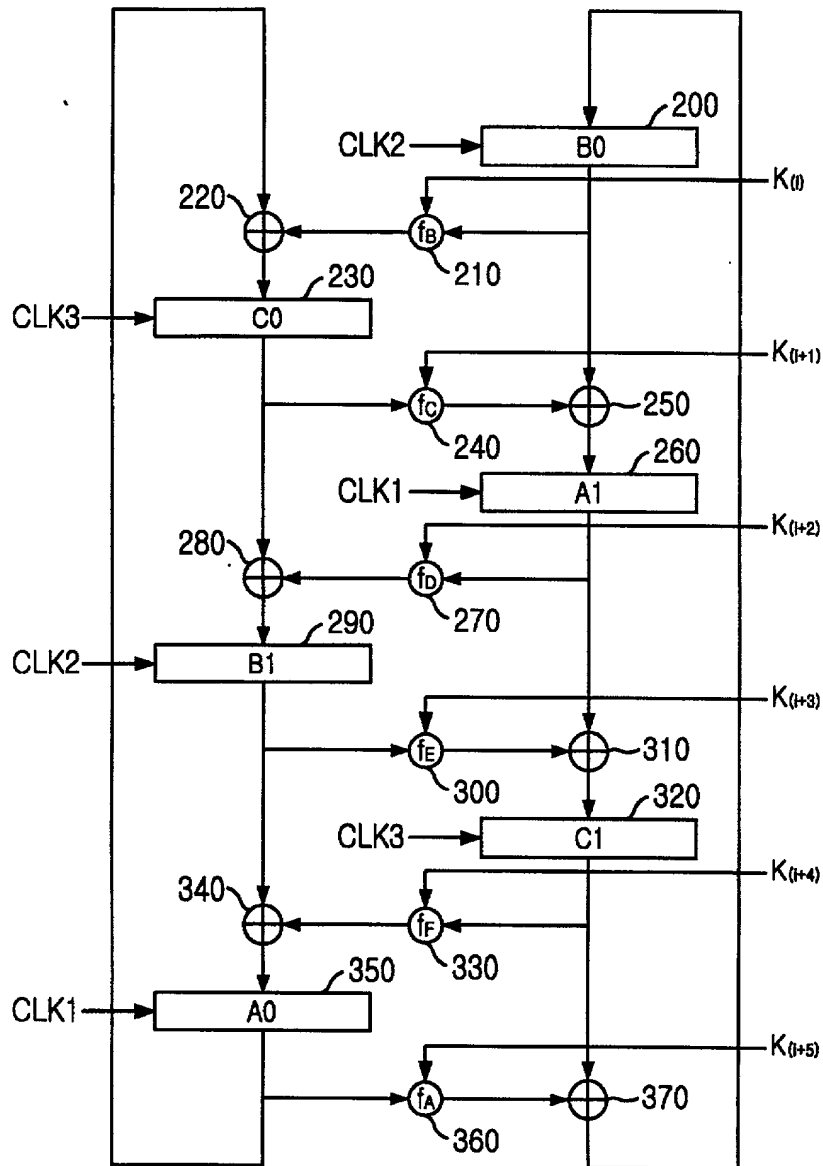


FIG. 3

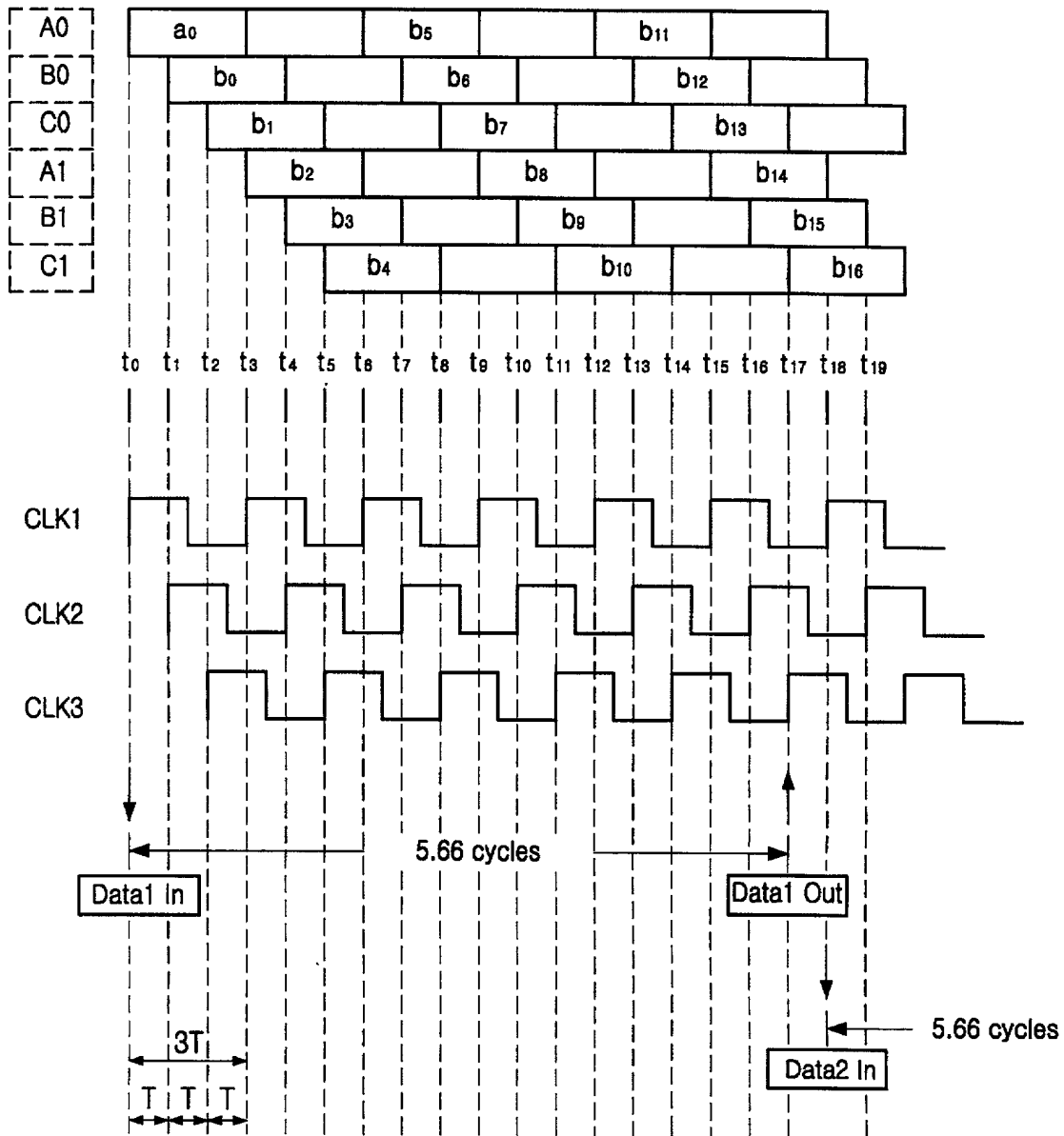


FIG. 4

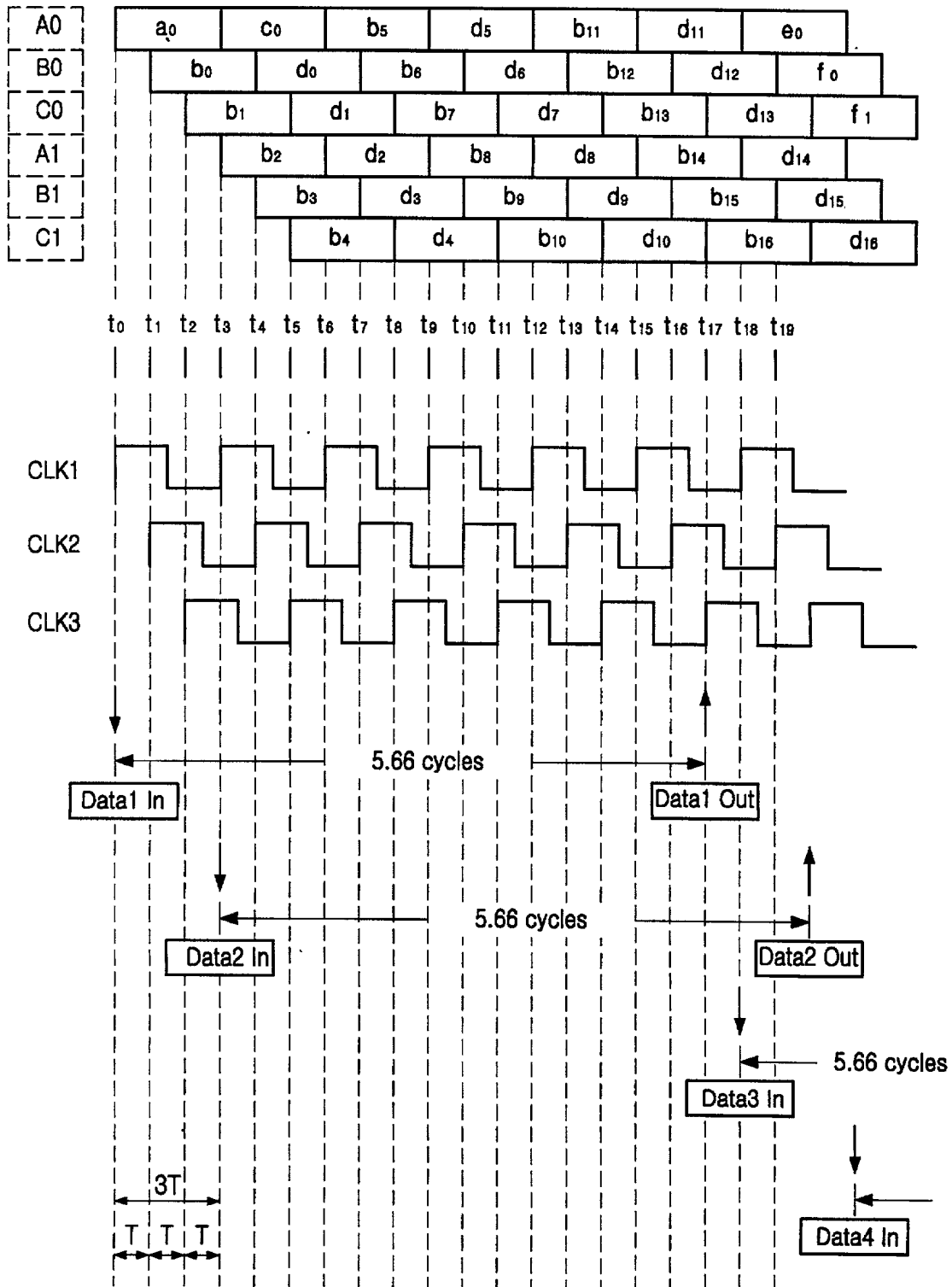


FIG. 5

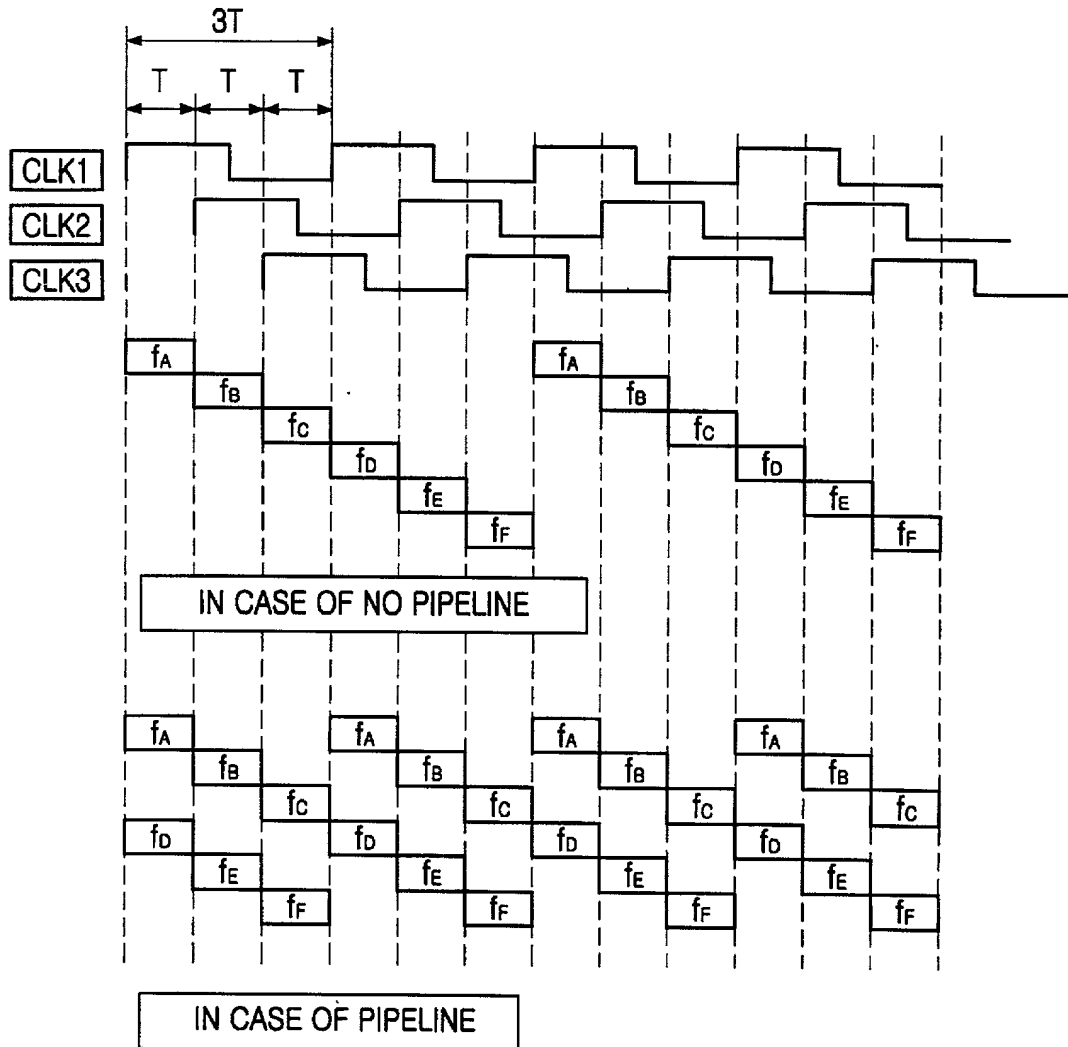


FIG. 6

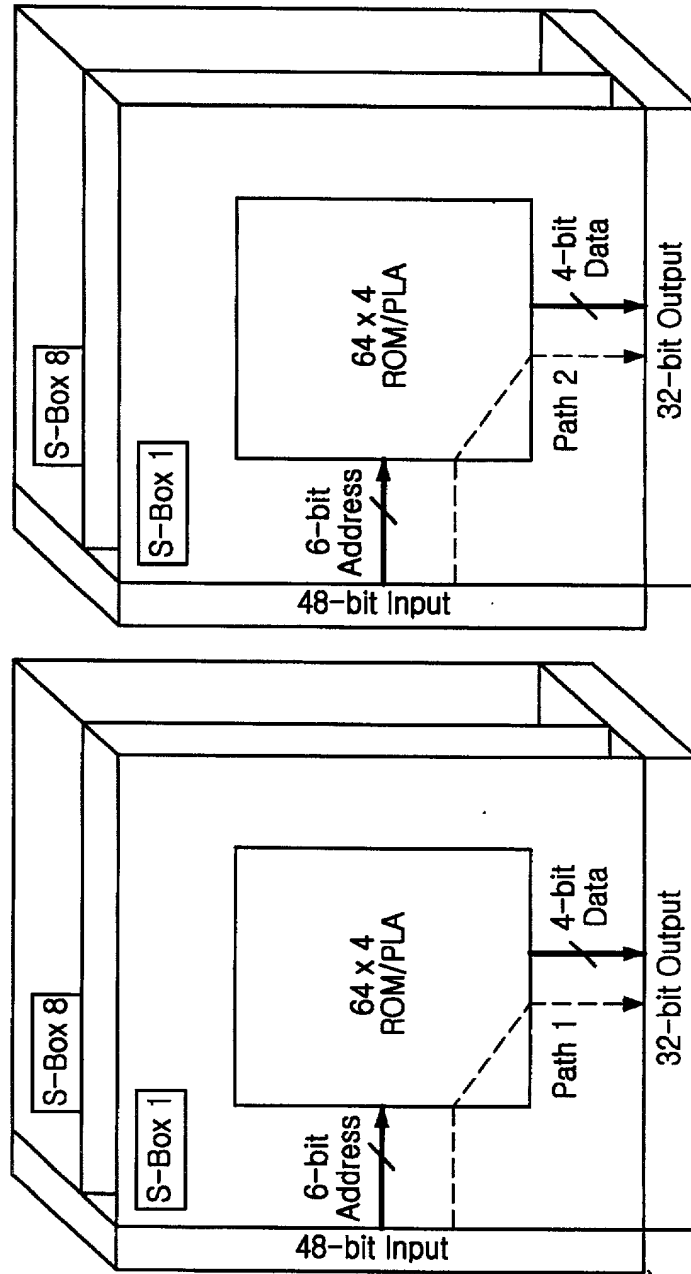


FIG. 7

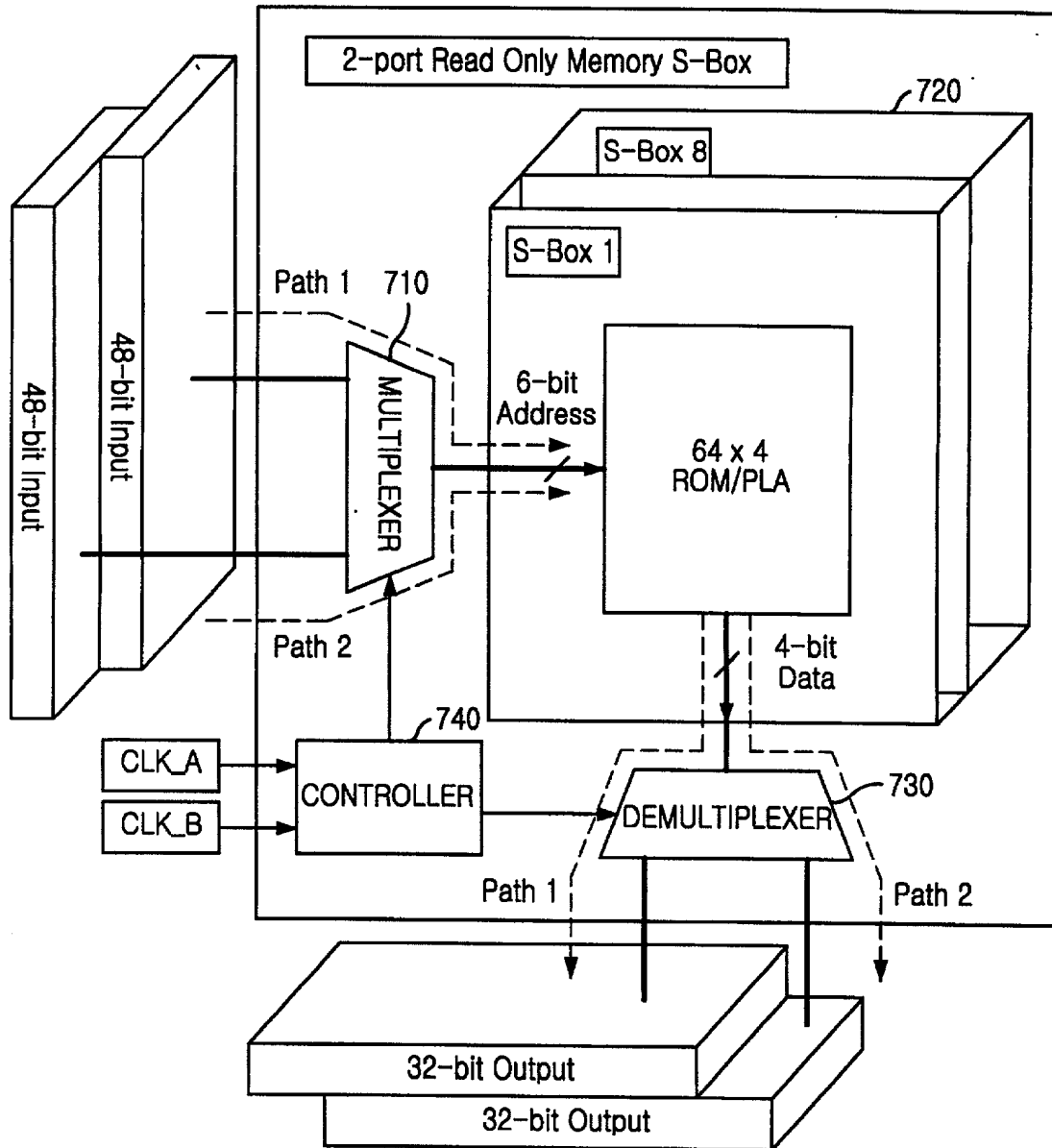
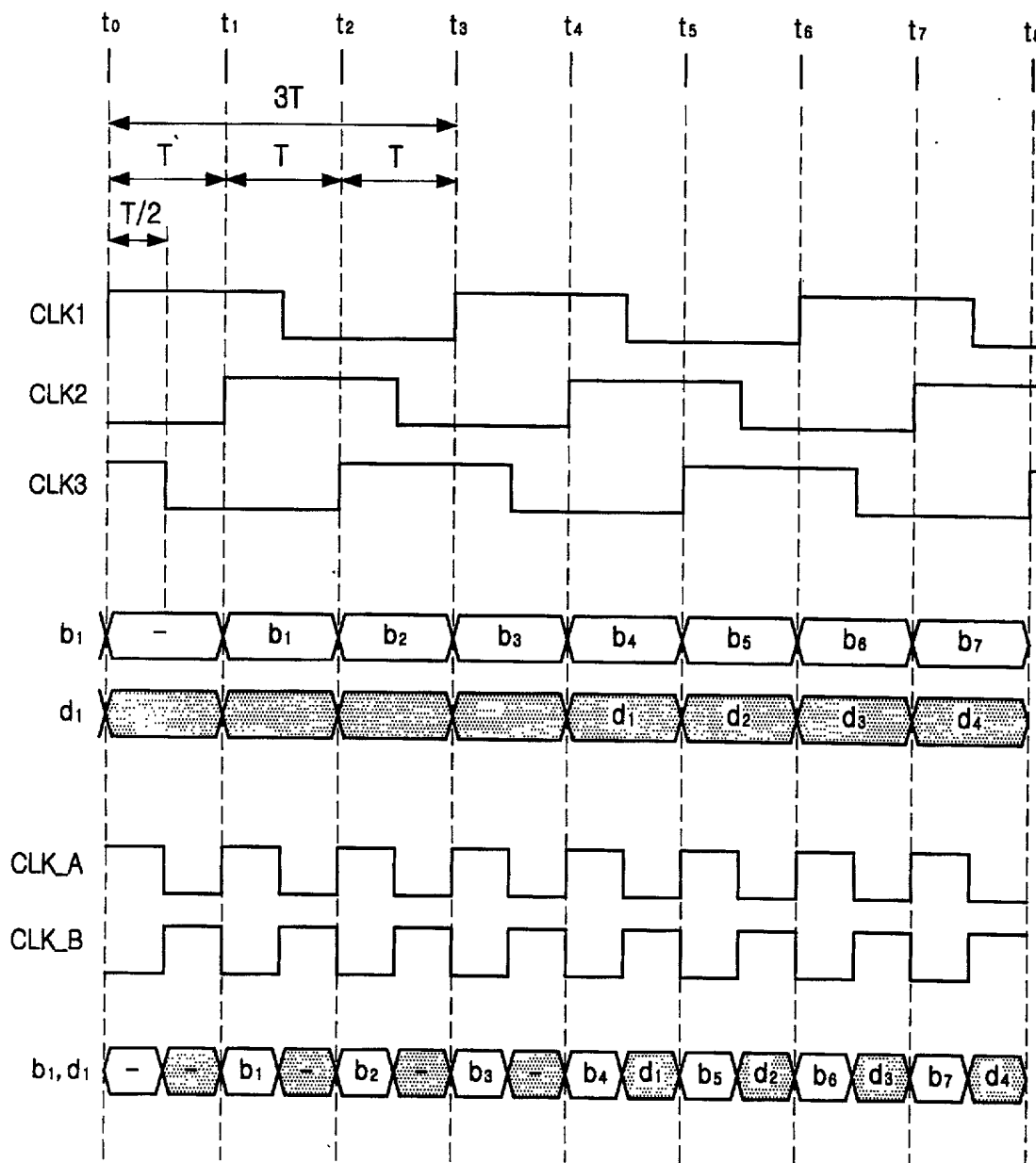


FIG. 8



□ : ACCESS TO S-Box THROUGH Path 1

■ : ACCESS TO S-Box THROUGH Path 2

-	b_1	b_2	b_3	b_4	b_5	b_6	b_7
-	$a_0 \oplus f(b_0, K_1)$	$b_0 \oplus f(b_1, K_2)$	$b_1 \oplus f(b_2, K_3)$	$b_2 \oplus f(b_3, K_4)$	$b_3 \oplus f(b_4, K_5)$	$b_4 \oplus f(b_5, K_6)$	$b_5 \oplus f(b_6, K_7)$

-	-	-	-	d_1	d_2	d_3	d_4
-	-	-	-	$c_0 \oplus f(d_0, K_1)$	$d_0 \oplus f(d_1, K_2)$	$d_1 \oplus f(d_2, K_3)$	$d_2 \oplus f(d_3, K_4)$